Marked-up Copy of the
AMENDED CLAIMS
(Corrected for Strikethrough Deletions)

1 (once amended). A method for encoding electronically readable cards having a card surface with visually readable indicia corresponding to an authorized user of said card and an electronically readable digital card data storage medium [permanently] affixed to said card, comprising the steps of:

deriving a first reference data element representative of random microstructure in said data storage medium;

deriving a second reference data element representative of a biometric aspect of said ~~authorized user~~ [individual]; [and]

storing ~~each~~ [one or both] of said first reference data element and said second reference data element [on] either ~~on~~ said card data storage medium or in an off-card data storage; ~~and~~

[whereby confidence in identification of a card user as the said authorized user is substantially increased by] verifying the first and said second reference data elements against ~~first and second~~ live data ~~elements~~ derived at a card transaction site in the course of a card transaction~~, wherein said second live data element includes biometric data derived from the live person of a card user presenting said card at the transaction site~~.

2 (once amended). The method of Claim 1 further comprising the steps of:

applying an encoding algorithm to said first reference data element and said second reference data element thereby to derive an encoded data element; and

~~storing~~ [recording] said encoded data element on ~~either~~ said ~~card~~ data storage medium ~~or in off-card data storage~~ for ~~retrieval in the course of a card transaction~~ [reading by an electronic card reader].

3 (original). The method of Claim 1 wherein said digital data storag medium is a magnetic stripe.

4 (original). The method of Claim 1 wherein said biometric aspect is a fingerprint and said second data element is derived from a scanned image of a finger of the said individual.

5 (original). The method of claim 1 wherein said visually readable indicia include alphanumeric indicia.

6 (original). The method of claim 1 wherein said visually readable indicia include photographic indicia.

7 (original). The method of claim 1 wherein said visually readable indicia include the name and a photograph of the said authorized user of the card.

8 (original). The method of Claim 1 further comprising the step of deriving a third reference data element representative of a scanned image of said indicia and storing said third reference data element on either said card data storage medium or in off-card storage; and verifying said third reference data element against a live third data element derived at a card transaction terminal in the course of a card transaction.

9. (once amended). The method of ~~Claim 2~~ [Claim 8] further comprising the steps of ~~deriving a third reference data element representative of a scanned image of said indicia and storing said third reference data element on either said card data storage medium or in off-card storage, and~~ also applying said encoding algorithm to said third data element with said first and said second data element thereby to factor said third data element in said encoded data element, ~~and verifying said third reference data element against a live third data element derived at a card transaction terminal in the course of a card transaction~~.

10 (original). The method of Claim 1 wherein said step of deriving a first reference data lement comprises the steps of scanning and digitizing microstructure of said magnetic

stripe and applying a first encoding algorithm to extract and encode features from digitized microstructure.

11 (original). The method of Claim 1 wherein said step of deriving a second reference data element comprises the steps of applying a live fingerprint to a fingerprint scanner, scanning and digitizing an image of said live fingerprint and applying a second encoding algorithm to extract and encode features from the digitized fingerprint image.

12 (original). The method of Claim 8 wherein said step of deriving a third reference data element comprises the steps of scanning and digitizing an image of some or all of said card face and applying a third encoding algorithm to extract and encode features from the digitized image of said card face.

13 (original). A method for verifying the authenticity of a mag-stripe card and verifying the identity of a card user presenting the card at a transaction site, said mag-stripe card having a card surface with visually readable indicia indicative of an authorized user of said card and an electronically readable digital data storage magnetic stripe permanently affixed to said card, said method comprising the steps of:

deriving a first reference data element representative of random microstructure in said data storage medium;

deriving a second reference data element representative of a biometric aspect of the person of said card user;

deriving a third reference data element representative of a scanned image of said visually readable indicia;

applying an encoding algorithm to said first reference data element, said second reference data element and said third reference data element thereby to derive an encoded data element;

recording said encoded data element on said data storage medium for reading by an electronic card reader;

comparing at least two of said first, said second and said third reference data elements against corresponding live data lements derived at a card transaction site in the course of a card transaction; and

authorizing a card transaction if said least two of said first, said second and said third reference data elements are validated by said comparing.

14 (original). The method of claim 13 wherein said step of verifying comprises the steps of:

providing a card reader at a transaction location;

presenting said mag-stripe card to said card reader;

reading said encoded data element on said magnetic stripe of said mag-stripe card;

applying a first decoding algorithm to said encoded data element to retrieve said first reference data element, said second reference data element and said third reference data element;

deriving a first live data element representative of random microstructure in said data storage medium of said mag-stripe card;

deriving a second live data element representative of a biometric aspect of the person presenting the card;

deriving a third live data element representative of a scanned image of said visually readable indicia;

comparing said first live, said second live and said third live data element against said first reference, said second reference and said third reference data element; and

authorizing a card transaction only if each said live data element is validated against the corresponding reference data element and denying the card transaction if any said live data element is not so validated.

15 (original). The method of claim 14 wherein said card reader comprises a DeLand enabled scanner and said step of deriving a first live data element comprises the steps of scanning and digitizing microstructure of said magnetic stripe and applying a first encoding algorithm to extract and encode features from digitized microstructure.

16 (original). The method of claim 14 wherein said card reader comprises a fingerprint scanner and said step of deriving a second live data element comprises the steps of applying a live fingerprint to said fingerprint scanner, scanning and digitizing an image of

said live fingerprint and applying a second encoding algorithm to extract and _ncod_ features from the digitized fingerprint image.

17 (original). The method of claim 14 wherein said card reader comprises a card face imager and said step of deriving a third live data element comprises the steps of scanning and digitizing an image of some or all of said card face and applying a third encoding algorithm to extract and encode features from the digitized image of said card face.

18 (original). A method for encoding a mag-stripe card for use in electronic transactions, said mag-stripe card having a card surface with visually readable indicia associated with an authorized user of said card and an electronically readable digital data storage magnetic stripe element permanently affixed to said card, said method comprising the steps of:

deriving a first reference data element representative of random microstructure in said data storage medium by scanning and digitizing microstructure of said magnetic stripe and applying a first encoding algorithm to extract and encode features from digitized microstructure;

deriving a second reference data element representative of a biometric aspect of the person of said card user by applying a live fingerprint of the authorized user of the card to a fingerprint scanner, scanning and digitizing an image of said live fingerprint and applying a second encoding algorithm to extract and encode features from the digitized fingerprint image;

deriving a third reference data element representative of a scanned image of said visually readable indicia by scanning and digitizing an image of some or all of said card face and applying a third encoding algorithm to extract and encode features from the digitized image of said card face;

applying a fourth encoding algorithm to said first reference data element, said second reference data element and said third reference data element thereby to derive an encoded data element; and

recording said encoded data lement on said mag-stripe lement.

19 (original). A method for verifying the authenticity of a mag-stripe card encoded as in Claim 18 and verifying the identity of a card user presenting said mag-stripe card at a transaction site, comprising the steps of:

providing a mag-stripe card reader at a transaction location, said card reader comprising a DeLand enabled scanner, a fingerprint scanner, and a card face imager;

presenting said mag-stripe card to said card reader;

reading said encoded data element on said mag-stripe element of said mag-stripe card;

applying a first decoding algorithm to said encoded data element to retrieve said first reference data element, said second reference data element and said third reference data element;

deriving a first live data element representative of random microstructure in said data storage medium by scanning and digitizing microstructure of said magnetic stripe and applying said first encoding algorithm to extract and encode features from digitized microstructure;

deriving a second live data element representative of a biometric aspect of the person of said card user by applying a live fingerprint of the card user to said fingerprint scanner of the card reader at the transaction location, scanning and digitizing an image of said live fingerprint and applying said second encoding algorithm to extract and encode features from the digitized fingerprint image;

deriving a third live data element representative of a scanned image of said visually readable indicia by scanning and digitizing an image of some or all of said card face with said card face imager at the transaction location and applying said third encoding algorithm to extract and encode features from the digitized image of said card face;

comparing said first live, said second live and said third live data element against said first reference, said second reference and said third reference data element; and

authorizing a card transaction only if each said live data element is validated against the corresponding reference data element and denying the card transaction if any said liv data element is not so validated.

20 (original). A method for improving the security of mag-stripe card based transactions, comprising the steps of:

providing a mag-stripe card having a card surface with visually readable indicia associated with an authorized user of said card and an electronically readable digital data storage magnetic stripe element permanently affixed to said card;

deriving either a first reference data element representative of random microstructure in said magnetic stripe element by scanning and digitizing microstructure of said magnetic stripe and applying a first encoding algorithm to extract and encode features from digitized microstructure or a third reference data element representative of a scanned image of said visually readable indicia by scanning and digitizing an image of some or all of said card face and applying a third encoding algorithm to extract and encode features from the digitized image of said card face;

deriving a second reference data element representative of a biometric aspect of the person of said authorized user by applying a live fingerprint of the authorized user of the card to a fingerprint scanner, scanning and digitizing an image of said live fingerprint and applying a second encoding algorithm to extract and encode features from the digitized fingerprint image;

applying a fourth encoding algorithm to said first reference data element and said second reference data element to derive an encoded data element;

recording said encoded data element on said mag-stripe element.

providing a mag-stripe card reader at a transaction location, said card reader comprising a scanner enabled for scanning and digitizing microstructure of said magnetic stripe, a fingerprint scanner, and a card face imager;

presenting said mag-stripe card to said card reader;

reading said encoded data element on said mag-stripe element of said mag-stripe card;

applying a first decoding algorithm to said encoded data element to retrieve said either first or third reference data element and said second reference data element;

deriving either a first live data element representative of random microstructure in said data storage medium by scanning and digitizing microstructure of said magnetic stripe and applying said first encoding algorithm to extract and encode features from digitized microstructur or a third live data element representative of a scanned image of

said visually readable indicia by scanning and digitizing an image of some or all of said card face with said card face imager at the transaction location and applying said third encoding algorithm to extract and encode features from the digitized image of said card face;

deriving a second live data element representative of a biometric aspect of the person of said card user by applying a live fingerprint of the card user to said fingerprint scanner of the card reader at the transaction location, scanning and digitizing an image of said live fingerprint and applying said second encoding algorithm to extract and encode features from the digitized fingerprint image;

comparing said either first or third live data element against said either first or third reference data element;

comparing said second live data element against said second reference data element; and

authorizing a card transaction only if each said live data element is validated against the corresponding reference data element and denying the card transaction if either said live data element is not so validated.

21 (original). The method of claim 20 wherein said card reader comprising a scanner enabled for scanning and digitizing microstructure of said magnetic stripe is a DeLand enabled card reader.

22 (original). A method for encoding electronically readable mag-stripe cards having a card surface with visually readable indicia corresponding to an authorized user of said card and a magnetic data storage mag-stripe element affixed thereto, comprising the steps of:

deriving a card authenticating reference data element representative of either random microstructure in said mag-stripe element or representative of a scanned image of said indicia

deriving a second reference data element representative of a biometric aspect of the authorized user; and

applying an encoding algorithm to said card authenticating reference data element and said second reference data element thereby to derive an encoded data element; and

recording said encoded data element on said data storage medium for reading by an electronic card reader at a card transaction location.

23 (original). A method for verifying the authenticity of a mag-stripe card encoded as in Claim 22 and verifying the identity of a card user presenting said mag-stripe card at a transaction site, comprising the steps of retrieving said card authenticating reference data element and said second reference data element by decoding said encoded data element and verifying each said reference data element against a corresponding live data element derived at a card transaction terminal in the course of a card transaction.

24 (new). A method for verifying the authenticity of electronically readable cards and the identity of a card user at a card transaction location, comprising the steps of:

providing a card having an electronically readable digital data storage medium permanently affixed to said card;

deriving a first reference data element representative of random microstructure in said data storage medium;

deriving a second reference data element representative of a biometric aspect taken by an electronic biometric scanner from the live person of an authorized user of said card;

storing each of said first reference data element and said second reference data element either on said card data storage medium or in off-card data storage;

deriving a first live data element at a card transaction location, said first live data element being representative of random microstructure in said data storage medium;

electronically deriving a second live data element at a card transaction site, said second live data element being representative of a biometric aspect taken by an electronic biometric scanner from the live person of a card user presenting said card at said card transaction site; and

verifying said first live data element against said first reference data element and said second live data element against said second reference data element.

25 (new). The method of Claim 24 further comprising the steps of:

applying an encoding algorithm to said first reference data element and to said second reference data element thereby to derive an encoded reference data element; and

recording said encoded reference data element either on said card data storage medium or in said off-card data storage.

26 (new). The method of Claim 25 wherein said step of verifying comprises the step of applying a decoding algorithm to said encoded reference data element at said card transaction site, thereby to recover said first reference data element and said second reference data element.

27 (new). The method of Claim 25 wherein said step of verifying comprises the steps of applying said encoding algorithm to said first live data element and said second live data element thereby to derive a encoded live data element and verifying said encoded live data element against said encoded reference data element.

28 (new). The method of any of Claims 24 through 27 wherein said digital data storage medium is a magnetic stripe.

29 (new). The method of any of Claims 24 through 27 wherein said biometric aspect is a fingerprint.

30 (new). The method of Claim 28 wherein each of said steps of deriving a first reference data element and a first live data element comprises the steps of scanning and digitizing microstructure of said magnetic stripe and applying a first encoding algorithm to extract and encode features from digitized microstructure.

31 (new). The method of Claim 29 wherein each of said steps of deriving a s cond r ference data element and a second live data element comprises the steps of applying a live fingerprint to a fingerprint scanner, scanning and digitizing an image of said live

fingerprint and applying a second ncoding algorithm to xtract and encode featur s from the digitized fingerprint image.

32 (new). A method for verifying the authenticity of a data storage card and verifying the identity of a card user presenting the card at a transaction site, said card having an electronically readable data storage medium affixed to said card, said method comprising the steps of:

deriving a first reference data element representative of random microstructure in said data storage medium;

deriving a second reference data element representative of a biometric aspect of the person of an authorized card user;

applying an encoding algorithm to said first reference data element and said second reference data element thereby to derive an encoded data element;

recording said encoded data element either on said data storage medium or in off-card data storage;

verifying said first and said second reference data elements against corresponding live data elements derived at a card transaction site in the course of a card transaction; and

authorizing a card transaction if said first and said second live data elements are validated by said verifying.

33 (new). The method of claim 32 wherein said step of verifying comprises the steps of:

providing at a transaction location a card reader enabled for deriving a first live data element representative of random microstructure in said data storage medium of said card and further enabled for deriving a second live data element representative of a biometric aspect of the live person of said card user present at said transaction location.

///

///

34 (new). The method of Claim 33 wherein said step of verifying further comprises the steps of:

presenting said card to said card reader;

reading said encoded data element;

applying a first decoding algorithm to said encoded data element to retrieve said first reference data element and said second reference data element;

deriving said first live data element representative of random microstructure in said data storage medium of said card; and

deriving a second live data element representative of a biometric aspect taken from a live person of the card user presenting the card at said transaction location.

35 (new). The method of claim 33 or claim 34 wherein said card reader comprises a DeLand enabled scanner and said step of deriving a first live data element comprises the steps of scanning and digitizing microstructure of said magnetic stripe and applying a first encoding algorithm to extract and encode features from digitized microstructure.

36 (new). The method of claim 33 or claim 34 wherein said card reader comprises a fingerprint scanner and said step of deriving a second live data element comprises the steps of applying a live fingerprint to said fingerprint scanner, scanning and digitizing an image of said live fingerprint and applying a second encoding algorithm to extract and encode features from the digitized fingerprint image.

37 (new). A method for verifying the authenticity of a data storage card having a magnetic stripe data storage medium and verifying the identity of a card user presenting the card at a transaction site, said method comprising the steps of:

deriving a first reference data element representative of random microstructure in said data storage medium by scanning and digitizing microstructure of said magnetic stripe storage medium and applying a first encoding algorithm to extract and encode features from digitized microstructure of said storage medium;

deriving a second reference data element r presentative of a biometric aspect of the person of an authorized user of said card;

storing each of said first and said second data elements either on said magnetic stripe data storage medium or in off-card data storage;

providing at a transaction location a card reader enabled for deriving a first live data element representative of random microstructure in said data storage medium of said card and further enabled for deriving a second live data element representative of a biometric aspect of the live person of a card user present at said transaction location.

presenting said card to said card reader;

deriving a first live data element representative of random microstructure in said data storage medium of said card;

deriving a second live data element representative of a biometric aspect taken from a live person of a card user presenting the card at said transaction location; and

verifying said first live data element against said first reference data element and said second live data element against said second reference data element.

38 (new). The method of claim 37 wherein said biometric aspect is a fingerprint and said card reader comprises a fingerprint scanner and said step of deriving a second live data element comprises the steps of applying a live fingerprint to said fingerprint scanner, scanning and digitizing an image of said live fingerprint and applying a second encoding algorithm to extract and encode features from the digitized fingerprint image.

39 (new). A method for verifying the authenticity of a data storage card having an electronically readable data storage medium and verifying the identity of a card user presenting the card at a transaction site, said method comprising the steps of:

deriving a first reference data element representative of random microstructure in said data storage medium by scanning and digitizing microstructure of said storage medium magnetic stripe and applying a first encoding algorithm to extract and encode features from digitized microstructure of said magnetic stripe;

providing a fingerprint scanner, applying a live fingerprint of an authorized user of said card to said fingerprint scanner, scanning and digitizing an image of said live fing rprint and applying a second encoding algorithm to extract and encode features from the digitized fingerprint image;

storing each of said first and said second data lements eith r in said data storage medium or in off-card data storage;

providing at a transaction location a card reader enabled for deriving a first live data element representative of random microstructure in said data storage medium of a card presented by a card user and further comprising a fingerprint scanner;

deriving a first live data element representative of random microstructure in said data storage medium by scanning and digitizing microstructure of said storage medium magnetic stripe and applying a first encoding algorithm to extract and encode features from digitized microstructure of said magnetic stripe;

applying a live fingerprint of a card user to said fingerprint scanner, scanning and digitizing an image of said live fingerprint and applying a second encoding algorithm to extract and encode features from the digitized fingerprint image;

retrieving said first reference data element and said second reference data element from said data storage on said card or said off-card data storage; and

verifying said first live data element against said first reference data element and said second live data element against said second reference data element.

40 (new). The method of Claim 39 wherein said first reference data element and said second reference data element are combined in and stored as an encoded reference data element.